UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,493	03/24/2004	B. John Oommen	BKCS 21.078 (331443-00004	8900

26304 7590 08/16/2007

KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER	
GERGISO, TECHANE	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
08/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/811,493	OOMMEN ET AL.	
	Examiner	Art Unit	
	Techane J. Gergiso T-G	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,6-28,30-36 and 41-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 6-28, 30-36, and 41-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/23/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a non-Final Office Action in response to the applicant's communication filed on June 07, 2007.

2. The applicant elected provisionally specious I with traverse for the election requirement mailed on February 20, 2007.

3. Claims 1, 6-28, 30-36, and 41-47 are pending.

Claim Objections

4. Claims 21-26, 28, 41-47 and 32-36 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim *should refer to other claims in the alternative only, and cannot depend from any other multiple dependent claim.* See MPEP § 608.01(n). Accordingly, the claims have not been further treated on the merits.

5. Claims 6, 20, 22-26, 30-36 and 41-47 are objected to because of the following:

Claim 6, 20, 22-26, 30-36 and 41-47 depend directly or indirectly on non-elected independent claims. Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claim 1 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1 is directed to "creating cipher text from plain text" This claimed subject matter lacks a practical application of judicial exception (law of nature, abstract idea, naturally occurring article/phenomenon) since it fails to produce a useful, and tangible result.

Specifically, the claimed subject matter does not produce **a useful result** because the **claimed subject matter fails to sufficiently reflect at least one practical utility** set forth in the descriptive portion of the specification. More specifically, while the described practical utility is directed to "*[0020-0021] It is a further object of an embodiment of the present invention to provide* ***an improved method of encoding and decoding data****, which permits the user to* ***obtain Statistical Perfect Secrecy in the cipher text****; and which* ***ensures that Statistical Perfect Secrecy in the cipher text*** *has been obtained. [0336-0337]* ***Serial Use of DDODE or RDODE with Traditional Encryptions; and both DDODE and RDODE can be used to enhance encryption Systems*** *by utilizing them serially, in conjunction with any, already existing, encryption mechanism.*" the subject matter relates ONLY to, **receiving a character of plaintext and**

traversing an Oommen-Rueda Tree between the root and the leaf and recording the assignment value of each traversed branch.

In addition, the claimed subject matter does not produce a **tangible result** because the claimed subject matter fails to produce a result that is limited to having a real world value rather than a result that may be interpreted to be abstract in nature as, for example, a thought, **a computation, or manipulated data**. More specifically, **the claimed subject matter provides receiving a character of plaintext and traversing an Oommen-Rueda Tree between the root and the leaf and recording the assignment value of each traversed branch**. This produced result remains in the abstract and, thus fails to achieve the required status of having real world value.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1 and 27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation " traversing an Oommen-Rueda Tree between **the root** and **that leaf** corresponding to **that character** of plaintext and recording **the Assignment Value** of **each branch** so traversed " in claim 1: lines 4-6. There is insufficient antecedent basis for this limitation in the claim (see the added bold and underlined emphasis).

Claim 1 recites the limitation "repeating steps b and c **until the plaintext has been processed.**" The scope of the claim is not clear because processing of the plain text does not explicitly specify when to stop repeating steps b and c.

Claim 27 recites the limitation "utilizing an Oommen-Rueda Tree having a structure corresponding to the Oommen-Rueda Tree initially utilized by **the Encoder** and utilizing **the same Branch Assignment Rule** as utilized by the Encoder to provide **the Assignment Values** for the branches depending from the root, traversing such Oommen-Rueda Tree from the root towards a leaf, the first character of cipher text determining the branch to then be traversed;" in claim 27: lines 3-9. There is insufficient antecedent basis for this limitation in the claim (see the added bold and underlined emphasis).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 6-20, 28 and 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chang et al. (hereinafter referred to as Chang; US. Pat. No.: 6,885,749) in view of Yoshiura et al. (hereinafter referred to as Yoshiura; US Pat. No: 6,411,714).

As per claim 1:

Chang discloses a method for creating cipher text from plaintext comprising the steps of (column 1: lines 25-60; scrambling; Huffman; data):

(a) receiving a character of plaintext (column 1: lines 25-60; receive data; receiver);

(b) traversing an Oommen-Rueda Tree between the root and that leaf corresponding to that character of plaintext and recording the Assignment Value of each branch so traversed (figure 8: 706: Huffman coder/decoder; column 3: lines 30-44);

(c) receiving a next character of plaintext (column 1: lines 25-60; receive data; receiver).

Chang does not explicitly disclose repeating steps b and c until the plaintext has been processed. Yoshiura in analogous art, however, disclose repeating steps b and c until the plaintext has been processed (figure 5: 1023-1025; column 13: lines 30-40; figure 7: 703-707; column 12: lines 5-14). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Chang to include repeating steps b and c until the plaintext has been processed. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do to provide a procedure of setting the correspondences between the symbols and the bit strings is changed in the course of the data processing and consequently, no repetitive pattern can make appearance in the encrypted data to yield the immunity of the encrypted data can be intensified as suggested by Yoshiura (in column 6: lines 25-30).

As per claim 6:

Chang discloses method for creating cipher text from plaintext, wherein the Assignment Value for at least one branch traversed is determined in accordance with a Branch Assignment Rule (column 3: lines 30-44).

As per claim 7:

Yoshiura discloses a method for creating cipher text from plaintext, wherein, when a member of the cipher text alphabet is under-represented in the cipher text generated thus far, the Branch Assignment Rule assigns that member of the cipher text alphabet to at least one of the branches being traversed between the root and the leaf so that that member of the cipher text alphabet is no longer as under-represented as before the assignment (column 11: lines 1-14; figure 4: 1011-1017; column 15: lines 40-60).

As per claim 8:

Yoshiura discloses a method for creating cipher text from plaintext wherein, when a member of the cipher text alphabet is under-represented in the cipher text generated thus far, the Branch Assignment Rule assigns that member of the cipher text alphabet more frequently than other members of the cipher text alphabet to the branches being traversed between the root and the leaf so that that member of the cipher text alphabet is no longer as under-represented as before the assignment (column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; figure 4: 1011-1017; column 15: lines 40-60; column 19: lines 1-12).

As per claim 9:

Yoshiura discloses a method for creating cipher text from plaintext wherein when, the cipher text alphabet is binary, the Branch Assignment Rule assigns a zero to the majority of branches being traversed between the root and the leaf when zero is under-represented in the cipher text generated thus far, and assigns a one to the majority of branches being traversed between the root and the leaf when one is under-represented in the cipher text generated thus far (column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; figure 4: 1011-1017; column 15: lines 40-60; column 19: lines 1-12).

As per claim 10:

Yoshiura discloses a method for creating cipher text from plaintext wherein, when the conditional frequency of one member of the cipher text alphabet given a particular sequence of members of the cipher text alphabet in the cipher text generated thus far, is under-represented in the cipher text generated thus far, the Branch Assignment Rule assigns that member of the cipher text alphabet to at least one of the branches being traversed between the root and the leaf so that the said conditional frequency of that member of the cipher text alphabet is no longer as under-represented as before the assignment (column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; figure 4: 1011-1017; column 15: lines 40-60; column 19: lines 1-12).

As per claim 11:

Yoshiura discloses a method for creating cipher text from plaintext wherein, when the conditional frequency of one member of the cipher text alphabet given a particular sequence of members of the cipher text alphabet in the cipher text generated thus far, is under-represented in

the cipher text generated thus far, the Branch Assignment Rule assigns that member of the cipher text alphabet more frequently than other members of the cipher text alphabet to the branches being traversed between the root and the leaf so that the said conditional frequency of that member of the cipher text alphabet is no longer as under-represented as before the assignment (column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; figure 4: 1011-1017; column 15: lines 40-60; column 19: lines 1-12).

As per claim 12:

Yoshiura discloses a method for creating cipher text from plaintext wherein, the Branch Assignment Rule assigns a member of the cipher text alphabet to at least one of the branches being traversed between the root and the leaf, such assignment being determined by comparing a number associated with the frequency of at least one member of the cipher text alphabet in the cipher text generated thus far, with a number associated with the output of a pseudo-random number generator (column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; figure 4: 1011-1017; column 15: lines 40-60; column 19: lines 1-12).

As per claim 13:

Yoshiura discloses a method for creating cipher text from plaintext wherein when the cipher text alphabet is binary, the Branch Assignment Rule assigns a member of the binary alphabet to at least one of the branches being traversed between the root and the leaf, such assignment being determined by comparing a number associated with the frequency of a member of the binary alphabet in the cipher text generated thus far, with a number associated with the

output of a pseudo-random number generator (column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; figure 4: 1011-1017; column 15: lines 40-60; column 19: lines 1-12).

As per claim 14:

Yoshiura discloses a method for creating cipher text from plaintext wherein the Branch Assignment Rule assigns a member of the cipher text alphabet to at least one branch being traversed between the root and the leaf, such assignment being determined by a number associated with the output of a pseudo-random number generator (column 3: lines 55-67; figure 4: 1012-1017; figure 3).

As per claim 15:

Yoshiura discloses a method for creating cipher text from plaintext wherein when the cipher text alphabet is binary, the Branch Assignment Rule assigns a member of the binary alphabet to at least one branch being traversed between the root and the leaf, such assignment being determined by comparing a number associated with the a pseudo-random number with a range equal to half the domain of the generator generating the pseudo-random number (column 3: lines 55-67; figure 4: 1012-1017; figure 3).

As per claim 16:

Yoshiura discloses a method for creating cipher text from plaintext wherein the Branch Assignment Rule assigns a member of the cipher text alphabet of cardinality R to at least one branch being traversed between the root and the leaf, such assignment being determined by

invoking at least two times (R minus 1) pseudo-random numbers, the domains of at least one of the pseudo-random numbers being related to the frequencies of the occurrences of the cipher text characters generated thus far, and the domain of at least one of the other of the pseudo-random numbers having a mean of i/R for the ith branch of each node encountered in the traversal, where i is the relative position of the branch quantified by a pre-specified ordering of the branches, and the Branch Assignment Rule being such that where the cipher text character associated with the ith branch in the said ordering is under-represented in the cipher text generated thus far, it is no longer as under-represented (column 3: lines 55-67; figure 4: 1012-1017; figure 3; column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; figure 4: 1011-1017; column 15: lines 40-60; column 19: lines 1-12).

As per claim 17:

Yoshiura discloses a method for creating cipher text from plaintext wherein when the cipher text alphabet is binary; the Branch Assignment Rule assigns a member of the binary cipher text alphabet to at least one branch being traversed between the root and the leaf, such assignment being determined by invoking at least two pseudo-random numbers, the domain of the first of these pseudo-random numbers being related to the frequency of the occurrence of zero in the cipher text, and the domain of a second of these pseudo-random numbers having a mean of 0.5, and the Branch Assignment Rule being such that when any character of the cipher text alphabet is under-represented in the cipher text generated thus far, it is no longer as under-represented (column 3: lines 55-67; column 8: lines 63-67; column 9: lines 1-10; column 11:

lines 1-14; column 12: lines 30-42; column 15: lines 40-60; column 19: lines 1-12; figure 3; figure 4: 1012-1017).

As per claim 18:

Yoshiura discloses a method for creating cipher text from plaintext wherein when the cipher text alphabet is binary, the Branch Assignment Rule assigns a member of the binary cipher text alphabet to at least one branch being traversed between the root and the leaf, such assignment being determined by comparing at least the output of two invoked pseudo-random numbers, the first of which has a domain having a mean between a number associated with the frequency of zeros and the quantity 0.5, and the second of which is a pseudo-random number having a domain whose mean is 0.5, and the Branch Assignment Rule being such that where any member of the cipher text alphabet is under-represented in the binary cipher text generated thus far, it is no longer as under-represented (column 3: lines 55-67; column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; column 12: lines 30-42; column 15: lines 40-60; column 19: lines 1-12; figure 3; figure 4: 1012-1017).

As per claim 19:

Yoshiura discloses a method for creating cipher text from plaintext wherein when the cipher text alphabet is binary, the Branch Assignment Rule assigns a member of the binary alphabet to at least one branch being traversed between the root and the leaf by utilizing at least two pseudo-random numbers, zero being assigned when a first pseudo-random number is less than a second pseudo-random number, where the generation of the second pseudo-random

number is bounded between a number associated with the frequency of zeros in the cipher text generated thus far and the quantity of one minus the said number associated with the frequency of zeros in the cipher text generated thus far (column 3: lines 55-67; column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; column 12: lines 30-42; column 15: lines 40-60; column 19: lines 1-12; figure 3; figure 4: 1012-1017).

As per claim 20:

Yoshiura discloses a method for creating cipher text from plaintext, comprising the further steps of, after at least one traversal of the Oommen-Rueda Tree, recalculating a number associated with the frequency weight of at least one of the nodes of the Oommen-Rueda Tee including the internal nodes and the leaves depending therefrom, and thereafter restructuring the Oommen-Rueda Tree in accordance with a Tee Restructuring Rule (column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; column 12: lines 30-42; column 15: lines 40-60).

As per claim 21:

Yoshiura discloses a method for creating cipher text from plaintext, comprising the further step of receiving first key data associated with an initial seed for at least one of the generators of the pseudo-random numbers utilized by the Branch Assignment Rule (column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; column 12: lines 30-42; column 15: lines 40-60).

As per claim 27:

Chang discloses a method for decoding cipher text, comprising the steps of:

(a) receiving a first character of cipher text (column 1: lines 25-60; descramble; Huffman; data; receive data; receiver);

(b) utilizing an Oommen-Rueda Tree having a structure corresponding to the Oommen-Rueda Tree initially utilized by the Encoder and utilizing the same Branch Assignment Rule as utilized by the Encoder to provide the Assignment Values for the branches depending from the root, traversing such Oommen-Rueda Tree from the root towards a leaf, the first character of cipher text determining the branch to then be traversed (figure 8: 706: Huffman coder/decoder; column 3: lines 30-44);

Chang does not explicitly disclose if a leaf has not been reached, utilizing the same Branch Assignment Rule as utilized by the Encoder to provide Assignment Values for the branches depending from the node that has been reached, receiving the next character of cipher text, and continuing to traverse the Oommen-Rueda Tree from the node that has been reached towards a leaf, the current symbol of cipher text determining the branch to then be traversed; when a leaf is reached, recording the plaintext character associated with the label of the leaf, the root becoming the node that has been reached for the purpose of further processing repeating the steps until all symbols of cipher text have been processed. Yoshiura in analogous art, however, disclose if a leaf has not been reached, utilizing the same Branch Assignment Rule as utilized by the Encoder to provide Assignment Values for the branches depending from the node that has been reached, receiving the next character of cipher text, and continuing to traverse the Oommen-Rueda Tree from the node that has been reached towards a leaf, the current symbol of

cipher text determining the branch to then be traversed; when a leaf is reached, recording the plaintext character associated with the label of the leaf, the root becoming the node that has been reached for the purpose of further processing repeating the steps until all symbols of cipher text have been processed (column 3: lines 55-67; column 8: lines 63-67; column 9: lines 1-10; column 11: lines 1-14; column 12: lines 30-42; column 15: lines 40-60; column 19: lines 1-12; figure 3; figure 4: 1012-1017).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Chang to include if a leaf has not been reached, utilizing the same Branch Assignment Rule as utilized by the Encoder to provide Assignment Values for the branches depending from the node that has been reached, receiving the next character of cipher text, and continuing to traverse the Oommen-Rueda Tree from the node that has been reached towards a leaf, the current symbol of cipher text determining the branch to then be traversed; when a leaf is reached, recording the plaintext character associated with the label of the leaf, the root becoming the node that has been reached for the purpose of further processing repeating the steps until all symbols of cipher text have been processed. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do to provide a procedure of setting the correspondences between the symbols and the bit strings is changed in the course of the data processing and consequently, no repetitive pattern can make appearance in the encrypted data to yield the immunity of the encrypted data can be intensified as suggested by Yoshiura (in column 6: lines 25-30).

As per claim 28:

Claim 28 is substantially similar to claim 27 except the limitation of creating an Oommen-Rueda Tree structure corresponding to the Oommen-Rueda Tree initially by the Encoder which is disclosed by Yoshiura (in figure 8). Therefore, claim 28 is rejected with the same rationale given above to reject claim 27.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art

Contact Information

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T-G

Techane Gergiso

Patent Examiner

Art Unit 2137

August 14, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER